I

(Resolutions, recommendations, guidelines and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters

(2007/C 139/01)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ([1]),

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ([2]), and in particular its Article 41,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. On 19 December 2005 and on 29 November 2006, the EDPS issued two opinions ([3]) on the Proposal of the Commission for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters. In these opinions, he underlined the importance of the proposal as an effective instrument for the protection of personal data in the area covered by Title VI of the EU-Treaty. In particular, in his second opinion the EDPS voiced his concerns that developments in the negotiations were leading towards a level of protection of personal data not only below the standards laid down in Directive 95/46/EC, but also incompatible with the more generally formulated Council of Europe Convention No 108 ([4]).

2. In January 2007, the German Presidency set out a series of basic points to revise the proposal, with a view to remove outstanding reservations and improve data protection in the third pillar ([5]). The revised draft proposal ([6]) was submitted to the EP for a second consultation on 13 April 2007.

([1]) OJ L 281, 23.11.1995, p. 31.
([2]) OJ L 8, 12.1.2001, p. 1.
([3]) The first Opinion can be found in the OJ C 47, 25.2.2006, p. 27; the second Opinion is available on EDPS website: www.edps.europa.eu
([4]) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe, 28 January 1981.
([5]) Council document 5435/07 of 18 January 2007, available at: register.consilium.europa.eu
([6]) Council document 7315/07 of 13 March 2007, available at: register.consilium.europa.eu

3. The substantive changes contained in the revised proposal, as well as its importance, call for a new opinion of the EDPS. This opinion will concentrate on the EDPS main concerns and will not revisit all the points made in his previous opinions, as these remain valid for this revised proposal.

II. THE NEW IMPETUS BY THE GERMAN PRESIDENCY

4. The EDPS welcomes the fact that the German Presidency is putting a lot of effort into the negotiations on this Council Framework Decision. It is common knowledge that the negotiations were blocked in Council, because of fundamental differences in opinion between the Member States on essential issues. It was therefore a wise decision of the Presidency to give these negotiations a new impetus by presenting a fresh text.

5. The fact that the German Presidency gave a new impetus to the negotiations is in itself very positive. However, after a thorough examination of the latest text, the EDPS is disappointed about the content. The text presented by the German Presidency does not fulfil expectations. This is for the following reasons:

— The text weakens the level of protection of the citizen, since a number of essential provisions for their protection which were included in the Commission proposal have been taken out.

— In many aspects the revised proposal even falls below the level of protection afforded by Convention 108. It is thus both unsatisfactory and will even be incompatible with international obligations of the Member States.

— The text adds new complexities to the dossier, since it covers data processing by Europol, Eurojust and the third-pillar Customs Information System, and it opens up the debate on the supervision on these bodies. Notably, this opinion will discuss whether a Council Framework Decision is an appropriate legal instrument for these topics.

— The legislative quality of the text is unsatisfactory. Apart from the choice of legal instrument, several provisions do not fulfil the requirements of the common guidelines for the quality of drafting of Community legislation ([7]). In particular, the text is not drafted clearly, simply and precisely, which makes it difficult for the citizens to identify their rights and obligations unambiguously.

— The low level of protection afforded by the proposal cannot properly serve the creation of an area of freedom, security and justice in which law enforcement information can be exchanged between police and judicial authorities disregarding national borders. Indeed, in the absence of a high and broadly applicable level of data protection, the proposal makes exchanges of information still subject to different national 'rules of origin' and 'double standards' that strongly affect efficiency in law enforcement cooperation while not improving the protection of personal data ([8]).

6. The EDPS is well aware of the difficulties in reaching unanimity in the Council. However, the decision-making procedure cannot justify a lowest common denominator approach that would hinder the fundamental rights of EU citizens as well as hamper the efficiency of law enforcement. In this context, it would be desirable that data protection expertise would be fully taken into account and that the recommendations made by the European Parliament in its resolutions ([9]) would be duly integrated.

([7]) Interinstitutional Agreement of 22 December 1998 on common guidelines for the quality of drafting of Community legislation (OJ C 73, 17.3.1999, p. 1). Examples can be found in chapter V of this opinion.

([8]) See for example, Article 14 on transfers to third countries and international bodies; Article 12(1)(d) on further processing of personal data; Article 10 on compliance with time-limits for erasure and review; Article 13 on compliance with national processing restrictions.

([9]) The European Parliament adopted its first resolution on the initial Commission proposal on 27 September 2006. A second resolution, on the revised proposal, is expected by June.

III. LEGAL FRAMEWORK AND FOCUS OF THIS OPINION

7. A Framework Decision on the protection of personal data in the third pillar is an essential element in the development of an area of freedom, security and justice. The growing importance of the police and judicial cooperation in criminal matters as well as the actions stemming from the Hague Programme ([10]) have highlighted the necessity of common standards in the protection of personal data in the third pillar.

8. Unfortunately, as repeatedly affirmed by the EDPS and other relevant actors ([11]), the existing instruments at European level are not sufficient. Council of Europe Convention 108, which is binding on Member States, lays down fundamental general principles of data protection, but, even though it must be interpreted in the light of the ECHR case law, does not provide for the necessary preciseness, as has been stated before by the EDPS on several occasions ([12]). Directive 95/46/EC, which integrated and specified the principles of Convention 108 with regard to the internal market, has been adopted already in 1995. This directive does not apply to activities which fall within the scope of the third pillar. For activities within the area of police and judicial cooperation all Member States have subscribed to Recommendation No R (87) 15 ([13]), which specifies Convention 108 to a certain extent for the police sector, but this is not a binding legal instrument.

9. In this context, Article 30(1)(b) of the EU-Treaty requires that common actions in the field of police cooperation entailing the processing of information by law enforcement authorities shall be subject to 'appropriate provisions on the protection of personal data'. Such appropriate provisions do not exist, in the absence of a Council Framework Decision with a satisfactory content.

10. A parallel can be easily drawn with the development of the internal market, where a high level of protection of personal data throughout the Community was considered to be an essential element to eliminate obstacles in the free circulation of goods, services, capitals, and persons, and led to the adoption of Directive 95/46/EC. By analogy, an area of freedom, security and justice in which information should freely flow between authorities dealing with law enforcement both at national and EU level requires a high and uniform level of protection of personal data in all Member States.

11. These considerations are in contrast with the current situation, in which there is not such a general framework and in which the provisions on the protection of personal data in the third pillar are 'sector specific' and dispersed in different legal instruments ([14]). Some recent proposals ([15]) confirm and enhance the already existing fragmentation of data protection provisions in this area and put at risk their consistency. Furthermore, the lack of a general framework affects the swift adoption of many proposals in the area of police and judicial cooperation.

12. For these reasons the EDPS has strongly supported the Commission proposal in his previous opinions and has put forward appropriate recommendations in order to improve the proposal which was needed to ensure an appropriate level of protection of the citizen. The EDPS has constantly held that a general framework for data protection in the third pillar must ensure a high and consistent standard of data protection, by building on data protection principles laid down by Convention 108 and Directive 95/46/EC, whilst also taking into account, where necessary, the specificities of law enforcement activities.

13. Consistency of this general framework with first pillar data protection principles is all the more important in a context in which the growing involvement of the private sector in law enforcement entails that personal data move from the first pillar to the third pillar (like in the case of PNR) or from the third

([10]) See also the Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union (OJ C 198, 12.8.2005, p. 1).

([11]) The Conference of European Data Protection Authorities, delivered an opinion on 24 January 2006, available as document No 6329/06 at register.consilium.europa.eu. The Council of Europe's Consultative Committee on the Convention for the Protection of Individuals with regard to automatic processing of personal data (T-PD) adopted on 20 March 2007 a paper outlining its initial remarks, which is available at: www.coe.int/dataprotection/

([12]) See, more recently, the opinion of the EDPS of 4 April 2007 on the initiative of 15 Member States with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, point 60.

([13]) Recommendation No R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, adopted on 17 September 1987 and available at: www.coe.int/dataprotection/

([14]) Such as the legal instruments regulating Europol, Eurojust, the third pillar Customs Information System.

([15]) Such as the recent initiatives concerning Europol, the Prüm Treaty and access by law enforcement to VIS database.

pillar to the first pillar. Relevant examples can be easily found: the use of 'no fly lists' including persons who should not be allowed on airplanes and established for law enforcement by airlines for purposes within the first pillar (commercial purposes as well as flight security), as well as the proposal on access by law enforcement authorities to the VIS database, established as an instrument of a common visa policy ([16]). Therefore, the EDPS stresses that data protection principles in the first pillar must apply also to the third pillar. However, the specificities of law enforcement activities may make additional or exceptional provisions necessary ([17]).

14. Appropriate, consistent and broadly applicable safeguards for data protection in the third pillar are essential not only to guarantee the fundamental right of data protection of individuals, but also to foster efficiency in law enforcement cooperation within the area of freedom, security and justice.

15. Against this background, this opinion assesses to what extent the current revised proposal lays down appropriate provisions on the protection of personal data, pursuant to Article 30(1)(b) of the EU-Treaty. In doing so, the EDPS will refer to some of the recommendations made in his previous opinions. This opinion will also assess whether the revised proposal respects the international obligations of Member states stemming from Council of Europe Convention 108 and ECHR case law, as well as the principles laid down in Recommendation No R (87) 15 on the use of personal data in the police sector. Furthermore, the EDPS will consider to what extent the provisions of the proposal would have an impact on efficiency in police and judicial cooperation.

IV. **MAIN CONCERNS**

IV.1. **Applicability to domestic processing of personal data**

16. The proposal now includes a recital stating that Member States will apply the rules of the Framework Decision to national data-processing, so that conditions for transmitting data *may* already be met when the data are collected (Recital 6a). This recital tries to address the concerns voiced not only by the EDPS in his previous opinions, but also by many other stakeholders. Indeed, the European Parliament, the Conference of data protection authorities, and even the Council of Europe's T-PD Consultative Committee — consisting of data protection representatives of European governments — have all made clear in various occasions that the applicability of the Framework Decision to domestic processing of personal data is an essential condition not only to ensure a sufficient protection of personal data but also to allow an efficient cooperation between law enforcement authorities ([18]).

17. However, the recital as such cannot impose an obligation which is not explicitly laid down in the provisions. Unfortunately, Article 1 (Purpose and scope) explicitly limits the applicability of the proposal to data exchanged between Member States or EU bodies, by guaranteeing that *'the basic rights and freedoms, and in particular the privacy, of data subjects are fully protected when personal data are transmitted […]'*.

18. Therefore, the current draft leaves to Member States' full discretion in the application of uniform data protection principles to domestic processing of personal data and does not bind Member States to implement the same common data protection standards, this all within an area of police and judicial cooperation, where internal borders must be lifted. Against this background, the EDPS highlights again that the possibility of having different levels of data protection in different Member States within the third pillar would be:

— inconsistent with the creation of an area of freedom, security and justice within which citizens move freely and with a proper approximation of the laws pursuant to Article 34(2)(b) of the EU-Treaty,

— not appropriate for the protection of personal data, in light of Article 30(1)(b) of the EU-Treaty,

([16]) See Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM(2005)600 final).
([17]) In the same line, see also the Explanatory memorandum of Recommendation No R (87) 15, point 37.
([18]) See documents mentioned in footnote 9.

— inefficient and unworkable for law enforcement authorities, which would be unduly burdened by unmanageable distinctions between domestic data and data transmitted or available for transmission, which in most cases will be part of the same file ([19]).

19. The EDPS strongly advises the legislator to extend the scope of applicability, by obliging — not only inviting — Member States to apply the Framework Decision to domestic processing of personal data. Moreover, there are no compelling legal arguments supporting the view that application to domestic data would not be allowed under Article 34 of the EU-Treaty.

IV.2. **Limitation of the further purposes for which personal data may be processed**

20. The principle of purpose limitation is one of the basic principles of data protection. In particular, Convention 108 states that personal data shall be '*stored for specified and legitimate purposes and not used in a way incompatible with those purposes*' (Article 5(b)). Derogations to this principle are allowed only insofar as they are provided for by law and constitute a necessary measure in a democratic society in the interests of, inter alia, the 'suppression of criminal offences' (Article 9). The case law of the European Court of Human Rights has made clear that these derogations shall be proportionate, precise and foreseeable, pursuant to Article 8, paragraph 2 of the European Convention on Human Rights ([20]).

21. In the current proposal, the provisions on purpose limitation are laid down both in Article 3 and Article 12. Article 3 allows further processing for purposes compatible with the one for which data were collected, and is thus, in this respect, in line with basic data protection principles.

22. However, Article 3 is far too broad and does not cover an appropriate limitation of the purposes for storage, also required by Article 5(b) of Convention 108, mentioned above. The general reference to the purposes of Title VI of the EU-Treaty can not be seen as specified and legitimate purposes. The purpose of police and judicial cooperation is not by nature legitimate ([21]), and certainly not specified.

23. Article 3 does not contain any derogation as would be possible pursuant to Article 9 of Convention 108. However, Article 12 of the proposal lays down a very broad and not clearly defined series of derogations to the purpose limitation principle in the context of personal data received from or made available by another Member State. In particular, the condition that derogations shall be necessary is not explicitly laid down in the article. Secondly, it is not clear which are the 'other […] administrative proceedings' for which Article 12(1)(b) allows processing of personal data collected and transmitted for a different purpose. Furthermore, Article 12(1)(d) allows processing for 'any other purpose' with the sole condition that the competent authority that has transmitted the personal data gives its consent. In this context, it shall be noted that the consent of the transmitting authority cannot be considered under any circumstances as replacing the consent of the data subject or providing legal grounds to derogate from the purpose limitation principle. Therefore, the EDPS would like to stress that this broad and open derogation does not fulfil the basic requirements of adequate data protection and even contradicts the basic principles of Convention 108. Therefore, the EDPS recommends the legislator to redraft the relevant provisions.

24. A last remark concerns Article 12(2), which allows the possibility that third pillar Council decisions take precedence over paragraph 1 where appropriate conditions are laid down for the processing of personal data. The EDPS notes that the formulation of this paragraph is very general and does not do justice to the nature of the Council Framework Decision as a *lex generalis* for police and judicial cooperation. This *lex generalis* should apply to all processing of personal data in this area.

25. The EDPS believes that the current provisions on further processing of personal data impinge on the basic purpose limitation principle and even fall below the existing standard laid down by Convention 108. Therefore, the EDPS recommends the legislator to redraft the relevant provisions in the light of the existing international data protection rules and of the relevant case law.

([19]) For a more detailed reasoning, see EDPS second opinion, points 11-13.
([20]) Among the consolidated case law in this domain, the most explicit case is Rotaru v. Romania.
([21]) It is not sufficient to start from the assumption that the police under all circumstances and in all cases operates within the limits of its legal obligations.

IV.3. **Adequate protection in the exchange of personal data with third countries**

26. Convention 108 also deals with transfers to third countries. The Additional protocol regarding supervisory authorities and transborder data flows lays down the general principle — subject to certain derogations — that transfer of personal data to third party is permitted only if that party 'ensures an adequate level of protection for the intended data transfer'. The principle of 'adequate protection' has been implemented and specified within several legal instruments of the European Union, not only in first pillar instruments on data protection, like Directive 95/46/EC ([22]), but also in legal instruments within the third pillar, such as the legal instruments establishing Europol and Eurojust.

27. Recital 12 of the current proposal states that, in case of transfer of personal data to third countries or international bodies, 'these data should, in principle, benefit from an adequate level of protection'. Furthermore, Article 14 allows personal data transmitted from another Member State to be transferred to third countries or international bodies when the transmitting authority has given its consent to the transfer in compliance with its national law. Therefore, the provisions of the proposal do not establish any need for adequate protection, nor foresee any common criteria or mechanisms in order to assess adequacy. This means that each Member State will assess at its own discretion the level of adequacy provided for by the third country or international organisation. As a consequence, the list of adequate countries and international organisations — to which a transfer is allowed — will considerably vary from Member State to Member State.

28. This legal framework would also hinder police and judicial cooperation. Indeed, law enforcement authorities of a Member State, when deciding on a request for a certain criminal file by a third country, will not only have to consider the adequacy of that country, but shall also take into account whether or not each of the other (up to 26) Member States that contributed to the file has given its consent, according to its own adequacy assessment of the relevant third country.

29. In this context, Article 27 of the proposal, on Relationship to agreements with third States, adds more uncertainty, stating that the Framework Decision is without prejudice to obligations and commitments incumbent upon Member States or upon EU by virtue of bilateral and/or multilateral agreements with third States. According to the EDPS, this provision should be clearly limited to existing agreements and should lay down that future agreements shall be in line with the provisions of this proposal.

30. The EDPS believes that current provisions on transfers of personal data to third countries and international organisations would not be appropriate to protect personal data as well as unworkable for law enforcement authorities. Therefore, the EDPS reiterates ([23]) the need to ensure an adequate level of protection when personal data are transferred to third countries or international organizations, and that mechanisms ensuring common standards and coordinated decisions with regard to adequacy are put in place. The same opinion has been expressed before by the European Parliament and the T-PD Committee of the Council of Europe.

IV.4. **Quality of data**

31. Article 5 of Convention 108 lays down the principles for ensuring the quality of personal data. Further details are provided in other non binding instruments like Recommendation No R (87) 15 and in its three evaluations carried out so far.

32. When comparing the current proposal with the aforementioned legal instruments, it is clear that some important guarantees, in some cases already provided by the Commission proposal, are lacking in the revised version:

— Article 3 of the proposal does not guarantee that data are obtained and processed fairly, as required by Article 5 of Convention 108.

([22]) With regard to this point, it should be noted that the Commission has recently stated, in its *Communication of 7 March 2007 on the follow-up of the Work Programme for better implementation of the Data Protection Directive*, that the rules laid down by Directive 95/46/EC in relation to transfers of personal data to third countries are substantially appropriate and need not to be modified.

([23]) See the concerns already expressed in the first opinion, paragraph IV.8, and in the second opinion, points 22-23.

— The proposal no longer includes any provisions laying down — as required by Principle 3.2 of Recommendation No R (87) 15 — that different categories of data are distinguished in accordance with their degree of accuracy and reliability and that data based on facts are distinguished from data based on opinions or personal assessments ([24]). The lack of such a common requirement could actually undermine the data being exchanged between police authorities as they will not be able to ascertain whether the data can be construed as 'evidence', 'fact', 'hard intelligence' or 'soft intelligence'. This could have the consequence of not only hampering security operations and intelligence gathering which rely on these distinctions but also making it more difficult for courts to secure convictions.

— There are no distinctions between different categories of data subjects (criminals, suspects, victims, witnesses, etc.) nor specific guarantees for data relating to non-suspects, contrary to Principle 2 of Recommendation No R (87) 15 and its evaluation reports ([25]). Again, these distinctions are not only necessary for the protection of the personal data of the citizen, but also for the ability of the recipients to be able to make full use of the data they receive. Without these distinctions, the receiving police services can not immediately use the data, but have first to ascertain how the data must be qualified and subsequently how they can be used and shared for different law enforcement purposes.

— The periodic review provided for by Article 6 does not ensure the periodic verification of data quality and that police files are purged of superfluous or inaccurate data and kept up to date, as required by Recommendation No R (87) 15 ([26]). The importance of such review for data protection is obvious, but again this is also vital for the efficient operation of police services. Old and out of date intelligence is at best useless and at worst can shift resources away from current priorities to matters which are not, and should not, be the focus of investigation.

— If personal data — transmitted from another Member State — are found to be inaccurate, there are no obligations or mechanisms to ensure their rectification in the originating Member State. Again the issue of accuracy is vital to the effective operation of the police and judiciary. If the quality of data cannot be guaranteed, it will harm the usefulness of data transfer as a tool for fighting crime across borders.

33. Against this background, the EDPS believes that the provisions relating to data quality of the current proposal are neither appropriate nor complete — specifically taking into account Recommendation No R (87) 15 which has been subscribed by all the Member States —, and they even fall below the level of protection required by Convention 108. It is also useful to recall once more that accuracy of personal data is in the interest of both the law enforcement itself as well as the individual ([27]).

IV.5. **Exchanges of personal data with non competent authorities and private parties**

34. According to Principle 5 (Communication of data) of Recommendation No R (87) 15, communication of personal data from law enforcement authorities to other public bodies or to private parties should only be permissible under specific and strict conditions. Such provisions, laid down in the initial Commission proposal and welcomed by the EDPS and the European Parliament, have been now deleted by the revised version. Therefore, the new text does not lay down any specific guarantees for transfers of personal data to private parties or non law enforcement authorities.

([24]) Point 52 of explanatory Memorandum to Recommendation states that *'[i]t should be possible to distinguish between corroborated data and uncorroborated data, including assessment of human behaviour, between facts and opinions, between reliable information (and the various shades thereof) and conjecture, between reasonable cause to believe that information is accurate and a groundless belief in its accuracy*'. See also the Second evaluation of the relevance of recommendation No R (87) 15 regulating the use of personal data in the police sector (1998), point 5.1.

([25]) See in particular, point 5.2 of the Second evaluation, mentioned above, and points 24-27 of the Third evaluation of Recommendation No R (87) 15 regulating the use of personal data in the police sector (2002).

([26]) See principle 7 (Length of storage and updating of data) and the Explanatory Memorandum, points 96-98.

([27]) Explanatory memorandum to Recommendation No R (87) 15, point 74.

35. In addition, access and further use by law enforcement authorities of personal data controlled by private parties shall be permitted only on the basis of well defined conditions and limitations. In particular, as the EDPS already mentioned in his previous opinions, access by law enforcement authorities shall be allowed only on a case-by-case basis, under specified circumstances, for specified purposes, and be under judicial control in the Member States. Recent developments, such as Directive 2006/24/EC ([28]) on data retention, the PNR agreement with the United States ([29]), and the access by law enforcement authorities to data held by SWIFT ([30]) confirm the fundamental importance of these guarantees. It is unfortunate that the current proposal does not provide for any specific guarantees on access and further use by law enforcement authorities of personal data collected by private parties.

36. Against this background, the EDPS notes that, with regard to exchanges of personal data with private parties and non competent authorities, the current proposal fails to comply with the principles of Recommendations No R (87) 15 and to address the fundamental issue of access and further use by law enforcement authorities of personal data controlled by private parties.

IV.6. **Other substantive points**

37. Besides the abovementioned main concerns, the EDPS would like to draw the legislator's attention to the following points, which in most of the cases have already been addressed in more details in his previous opinions:

— **Special categories of data**. Article 7 of the revised proposal contradicts the in-principle prohibition laid down by Article 6 of Convention 108. Furthermore, it fails to refer to personal data relating to criminal convictions, which are undoubtedly very relevant in the context of police and judicial cooperation, and does not provide for specific safeguards with regard to biometric data and DNA-profiles.

— **Automated individual decisions**. EDPS welcomes that Article 8 integrates this provision into the revised proposal.

— **Logging and documentation**. Article 11, in order to be effective for the purposes of verification of the lawfulness of data processing, shall lay down appropriate mechanisms for logging or documenting not only all transmissions of data, but also *all accesses* to data.

— **Right to be informed**. Article 16 is incomplete, since it does not mention information about the identity of the controller and the recipients. Furthermore, Recital 13 ('[…] it may be necessary to inform data subjects […]') depicts information as a mere possibility rather than a basic obligation of the controller.

— **Right of access**. Article 17 is incomplete, since access shall include also the *purposes* for which data are processed and communication in an *intelligible form*. Furthermore, exceptions laid down by paragraph 2 — such as the case when access would 'otherwise be detrimental to national interests' — are too broad and unforeseeable. Lastly, there is no mechanism ensuring that the appeal to the supervisory authority results in granting access, when it had been unlawfully denied.

V. **NEW ISSUES RAISED BY THE REVISED PROPOSAL**

38. The revised proposal includes as a fully new element, in comparison with the Commission proposal. It covers activities by European institutions and bodies in the third pillar (Article 1(2) of the proposal). According to the 20th Recital, this includes data processing by Europol, Eurojust and the third pillar Customs Information System. Article 1(2) does not only mention European bodies but also institutions, which means that for instance data processing within the Council should be subject to the Council

([28]) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105, 13.4.2006, p. 54).

([29]) Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (OJ L 298, 27.10.2006, p. 29).

([30]) See Working Party 29 Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf, and EDPS Opinion on the role of the European Central Bank in the SWIFT case, available at EDPS website.

Framework Decision. It is not clear whether the drafters intended such a wide scope, or that they intended to limit the application to the three bodies mentioned in the 20th Recital. It would in any event be needed to specify the text, in order to avoid legal uncertainty.

39. This leads to a more general remark. According to the EDPS, it is of utmost importance that an appropriate level of data protection is guaranteed throughout the whole third pillar, since only under such condition a free exchange of information within an area of freedom, security and justice without internal borders would be facilitated in a sufficient manner. This includes applying the general framework on data protection to the European bodies in the third pillar. The EDPS underlined this need earlier in Part IV of his Opinion on the proposal for a Council Decision on Europol.

40. However, for reasons of effective law making the EDPS has serious doubts whether the present Council Framework Decision should cover the activities of the European bodies that operate in the third pillar. The first argument against this wide scope has to do with legislative policy. The EDPS fears that including the European bodies in the present text would run the risk that the discussions in Council will concentrate on this new element, instead of on the substantive provisions on data protection. It will complicate the legislative process. The second argument is of a legal nature. At first sight, it seems that a Council Framework Decision — an instrument which is comparable to a directive under the EC-Treaty — is not an appropriate legal instrument to regulate the rights and obligations of European bodies. Article 34 of the EU-Treaty introduces this instrument for the approximation of the laws and regulations of the Member States. In any event, there is a serious risk that the legal basis will be challenged during the legislative process, or afterwards.

41. The EDPS has a similar view, also with regard to the legal instrument chosen, on Article 26 of the draft, which foresees the establishment of a new joint supervisory authority, replacing the existing authorities that supervise the data processing within third pillar bodies. By itself, the intention to set up such an authority may seem logical. It might lead to an even more efficient system of supervision, and further ensure consistency of the level of protection within the bodies established under the third pillar.

42. However, at this moment there is no immediate need for such a new supervisory body. The supervision itself functions satisfactorily. Moreover, the president of Eurojust has put forward objections against application of this system of supervision to Eurojust. Without entering into the substance of these objections, it is clear that adding the subject matter of supervision on EU-bodies to the Council Framework Decision would make the legislative process even more difficult. In addition, this approach would not be consistent with other proposals in this area that are presently on the table ([31]) or have been recently adopted ([32]).

43. In short, the EDPS advises not to add provisions relating to data processing by EU-bodies to the text of the Council Framework Decision. The EDPS gives this advice for reasons of effective law making. It is important that all efforts in Council will be concentrated on the substantive provisions of data protection in order to give the citizen the necessary protection.

VI. **CONCLUSIONS**

44. The EDPS welcomes the new impetus given by the German Presidency. Adopting a general framework for data protection in the third pillar is essential, as the EDPS and other relevant actors have already highlighted in several occasions, in order to support the development an area of freedom, security and justice in which citizens' right to protection of personal data is uniformly guaranteed and cooperation between law enforcement authorities can take place disregarding national borders.

45. However, the revised proposal does not meet either of these objectives. Indeed, in the absence of a high and broadly applicable level of data protection, the proposal makes exchanges of information still subject to different national 'rules of origin' and 'double standards' that strongly affect efficiency in law enforcement cooperation while not improving the protection of personal data.

([31]) Such as the recent Commission proposal on establishing the European Police Office, COM(2006)817 final.
([32]) Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 381 of 28.12.2006, p. 4).

46. To give a concrete example, this would mean that a law enforcement body at national or EU level, when dealing with a criminal file — consisting of information originating from various national, other Member States' and EU authorities — would have to apply different processing rules for different pieces of information depending on whether: personal data have been collected domestically or not; each of the transmitting bodies has given its consent for the envisaged purpose; the storage is compliant with time limits laid down by applicable laws of each of the transmitting bodies; further processing restrictions requested by each of the transmitting bodies do not prohibit the processing; in case of a request from a third country, each transmitting body has given its consent according to its own evaluation of adequacy and/or international commitments. In addition, citizens' protection and rights will vary enormously and be subject to different broad derogations depending on the Member State where processing takes place.

47. Furthermore, the EDPS regrets that the legislative quality of the text is unsatisfactory and that the proposal adds new complexities to the dossier, by extending the applicability of the Framework Decision to Europol, Eurojust and the third-pillar Customs Information System as well as proposing the creation of a Joint Supervisory Body on the basis of an inappropriate legal instrument.

48. The EDPS is concerned because the current text takes out essential provisions for the protection of personal data which were included in the Commission proposal. By doing so, it significantly weakens the level of protection of the citizens. Firstly, it fails to provide the added value to Convention 108 which would make its provisions appropriate from a data protection point of view, as required by Article 30(1) of the EU-Treaty. Secondly, it also fails to meet in many aspects the level of protection required by Convention 108. Therefore, the EDPS believes that this proposal would need substantial improvements before it could be the basis for the discussion of an adequate general framework on data protection in the third pillar. These improvements should make sure that this general framework:

    — Provides added value to Convention 108, by laying down the appropriate provisions on the protection of personal data required by Article 30(1) of the EU-Treaty.
    — Is applicable to domestic processing of personal data by law enforcement authorities.
    — Is consistent with first pillar data protection principles, whilst also taking into account, where necessary, the specificities of law enforcement activities.
    — Is in line with the principles laid down by Convention 108 and Recommendation No R (87) 15, in particular with regard to:
        — Limitation of the further purposes for which personal data may be processed.
        — Quality of data, including distinction between different categories of data subjects (criminals, suspects, victims, witnesses, etc.), assessment of the different degree of accuracy and reliability of personal data, mechanisms to ensure periodic verification and rectification.
        — Conditions for transfers of personal data to non competent authorities and private parties, as well as for access and further use by law enforcement authorities of personal data controlled by private parties.
    — Ensures adequate protection in the exchange of personal data with third countries, also with regard to international agreements.
    — Addresses the other points mentioned in this as well as previous EDPS opinions.

49. The EDPS is well aware of the difficulties in reaching unanimity in the Council. However, the decision making procedure cannot justify a lowest common denominator approach that would hinder the fundamental rights of EU citizens as well as hamper the efficiency of law enforcement.

Done at Brussels, 27 April 2007.

Peter HUSTINX

European Data Protection Supervisor